SOPHOS

PureMessage for Microsoft Exchange
startup guide

Product version: 3.1
Document date: May 2010

Contents

1 About this guide....3
2 Planning your PureMessage deployment....4
3 Installing PureMessage....6
4 Starting and configuring PureMessage....13
5 Setting up alerts....16
6 Ensuring anti-virus scanning is enabled....17
7 Blocking files which may contain threats....18
8 Blocking spam....19
9 Scanning Exchange Message Stores....21
10 Dealing with quarantined items....23
11 Monitoring system activity....26
12 Uninstalling PureMessage....28
13 Appendix A: Deploying PureMessage to Exchange clusters....29
14 Appendix B: How to configure upstream (trusted) relays....36
15 Appendix C: How does PureMessage route mail?....37
16 Appendix D: About PureMessage mail scanning....38
17 Appendix E: Filtering attachments containing unwanted content....41
18 Appendix F: Database Mirroring....43
19 Glossary....48
20 Technical support....50
21 Legal notices....51

1 About this guide

This guide tells you how to do the following:

- install PureMessage for Microsoft Exchange
- start PureMessage
- integrate PureMessage with Active Directory
- set up alerts
- ensure that anti-virus scanning is enabled
- block file types that may contain threats
- set up spam blocking (if your license permits)
- set up Exchange store scanning
- deal with quarantined items
- enable end-users to access and deal with quarantined items
- monitor system activity

To upgrade, see the *PureMessage for Microsoft Exchange upgrade guide* instead of this guide.

2 Planning your PureMessage deployment

This section provides best-practice advice about installing PureMessage on different network topologies.

2.1 Deploying PureMessage to Exchange servers

You can deploy PureMessage to single or multiple Exchange servers.

2.1.1 Deploying PureMessage to a single Exchange server

If your network has only one Exchange server, deploying PureMessage is straightforward: install PureMessage on the Exchange server and configure it according to your email security policy.

2.1.2 Deploying PureMessage to multiple Exchange servers

PureMessage can protect both front-end (edge, hub transport) servers and back-end (mailbox) servers.

Note: It is recommended that you perform anti-spam scanning on the edge server to filter spam, and install the anti-virus only version of PureMessage on your back-end servers that do not require anti-spam scanning.

Example: Exchange 2007/2010 roles

PureMessage can be installed on a single Exchange server carrying out multiple Exchange roles, but can also be installed on Exchange servers with dedicated roles as illustrated below.

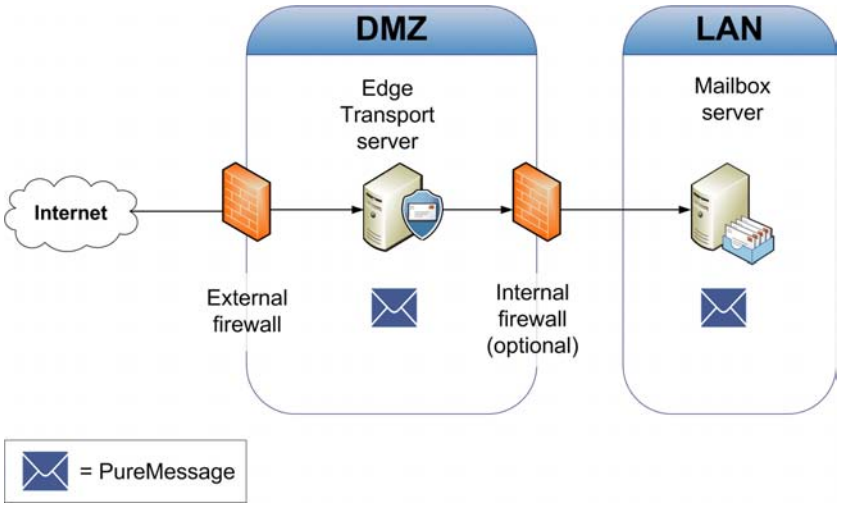


Figure 1: Exchange 2007/2010 roles

2.2 Deploying PureMessage to an IIS SMTP gateway

You can significantly reduce the scanning overhead on your back-end email servers (both Exchange and non-Exchange) by deploying PureMessage in a gateway role on a front-end server to filter the majority of unwanted email from inbound SMTP traffic.

Example: SMTP gateway role

The figure below shows PureMessage installed on a Windows IIS SMTP server upstream from a group of Exchange 2003 servers.

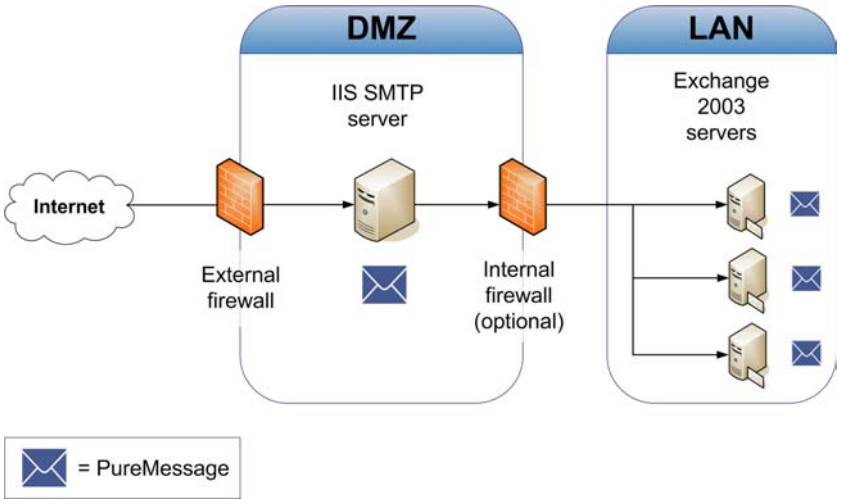


Figure 2: SMTP gateway role

In this example, PureMessage performs the following functions on the front and back-end servers:

Front-end server: SMTP gateway	Back-end servers: Exchange 2003
Scans inbound SMTP traffic and removes malware and spyware	Scans outbound and internal emails and filters malware and spyware. Scans Exchange private and public information stores and filters malware and spyware
Scans inbound SMTP traffic and deletes high-scoring spam	Scans inbound emails and quarantines emails with a medium to high spam score
Removes unwanted file types from inbound SMTP traffic	Filters content within inbound, outbound and internal emails
Scans inbound SMTP traffic and discards emails sent to non-existent recipients	

3 Installing PureMessage

This section describes how to install PureMessage.

Note: If you are installing PureMessage to an Exchange cluster, check the system requirements and then go to *Appendix A: Deploying PureMessage to Exchange clusters* (page 29).

The PureMessage product consists of two components:

- The PureMessage service.
- The PureMessage administration console.

This section tells you how to install both on a single server and also how to install a separate administration console in order to manage remote PureMessage servers.

Installation involves the following steps:

- Checking the system requirements.
- Preparing for installation.
- Preconfiguring updates (Sophos Enterprise Console customers only).
- Installing PureMessage.
- Installing a PureMessage console on a separate computer (optional).

3.1 System requirements

For system requirements, see the system requirements page of the Sophos website (*http://www.sophos.com/products/all-sysreqs.html*).

If you are currently using MSDE or SQL Server 2000 database, it is recommended that you upgrade to SQL Server 2005 or later (any edition) for optimized performance.

For details on how to upgrade existing MSDE or SQL Server 2000 database, see *http://www.sophos.com/support/knowledgebase/article/31157.html*.

3.2 Preparing for installation

Note:

- PureMessage installs Microsoft .NET Framework 3.5 SP1 as a prerequisite. This component has known issues related to Exchange Web services. After installing PureMessage, it is recommended to install the update for .NET Framework provided in Microsoft knowledgebase article 959209 (*http://support.microsoft.com/kb/959209*). If you are using the Microsoft Windows Server Update Services (WSUS) this update will be applied automatically.
- If you are running Windows 2008 or Windows 2008 R2 Server, read *http://www.sophos.com/support/knowledgebase/article/109664.html* before installing PureMessage.

- If you are installing PureMessage on a Windows Essential Business Server (EBS), SQL 2008 Express will not be installed as it is not recommended by Microsoft. In this case, you should either use a database located on another machine (remote database) or install SQL 2005 on the EBS machine before installing PureMessage.

Before you begin installation, you should do the following:

- Read the *PureMessage for Microsoft Exchange release notes* for details of new features and known issues.
- Make sure that a backup has been made of the mailboxes and databases.
- PureMessage installation may require a restart, so schedule the installation for a time when restarting the server will cause the least inconvenience.

If you want to use spam blocking:

- Make sure that you have a valid anti-spam license and download credentials from Sophos so that you can download anti-spam updates.
- Make sure that PureMessage is installed on a computer with Internet access, as anti-spam updates are only available direct from Sophos.
- If you use Sophos Enterprise Console to protect your PureMessage server, make sure that the server is configured to download anti-spam updates directly from Sophos as described in *Preconfiguring updates* (page 7).

If you are installing PureMessage on multiple servers, make sure that your SQL server is set up for remote access. See the *PureMessage for Microsoft Exchange release notes* for further details.

3.3 Preconfiguring updates

If you use PureMessage for spam blocking, it needs to update regularly with the latest rules for detecting spam. These spam rules can only be downloaded directly from Sophos via the internet.

If you are going to install PureMessage on a computer that does not already have Sophos Anti-Virus installed, updating will be set up for you and you need take no further action. Go to *Installing PureMessage* (page 8).

If you are going to install PureMessage on a computer already running Sophos Anti-Virus and managed by Sophos Enterprise Console, you must follow the instructions below.

Note: You will need the username and password that you use for downloads from the Sophos website.

1. Go to the computer running Enterprise Console and start Enterprise Console.
2. Ensure that the computer(s) running PureMessage are in a group of their own or have their own policy setting.
3. Create an Updating policy (or edit the existing policy) for the group.
4. In the **Updating Policy** dialog box, click the **Secondary server** tab.

5. In the **Secondary server** dialog box, select **Specify secondary server details**. Then in the **Address** field, click the drop-down arrow and select **Sophos**. Enter your username and password.
6. If necessary, enter proxy details.

You have preconfigured updating and are ready to install PureMessage.

3.4 Installing PureMessage

To install PureMessage, do as follows:

Note: The following services (and any dependent services) may be stopped and started during the installation of PureMessage:

- Internet Information Services (IIS)
- Microsoft Exchange Transport service
- Microsoft Exchange Information Store service
- Distributed File System Replication (DFSR) service

1. Log on to the server as an administrator, based on your environment:
   - If you are in a domain, log on with domain administrative privileges.
   - If you are in a workgroup, log on with local administrative privileges.

   Note: When installing on Exchange 2010, make sure you are a member of the Exchange Organization Administrators group.

   If installing from a Sophos PureMessage CD, run the CD and follow the on-screen links. Then go to step 4.
2. Visit the Sophos product download page at *http://www.sophos.com/support/updates/*. You will need credentials to download products and documentation.
3. Browse to the PureMessage page and download the PureMessage for Microsoft Exchange installer package you require. Choose **Anti-virus and anti-spam** or **Anti-virus only** (as your license permits).
4. Using Windows Explorer, browse to your download folder and start the installer package. The installation wizard begins.

   Note: Ensure that the installer is not run from a network share.
5. In the **Welcome** dialog box, click **Next**.
6. In the **License Agreement** dialog box, read the agreement. If you agree with the terms, click **I accept the terms of the license agreement** and click **Next**.
7. In the **Select Features** dialog box, select the components you want to install and click **Next**.
8. In the **Choose Destination Location** dialog box, you see the default folder where PureMessage will be installed. If you want to install it in a different folder, click **Browse** and select a folder. Click **Next**.

9. In the **Sophos Download Credentials** dialog box, enter the **User name** and **Password** that were supplied by Sophos.

   If you access the internet via a proxy, click **Proxy Details** and enter your proxy settings. Otherwise, click **Next**.

10. If the server is part of a SCC/CCR cluster, in the **PureMessage Cluster Settings** dialog box, select the cluster properties to be used for the PureMessage virtual server instance.

    Note: The PureMessage cluster settings dialog box is displayed only if the server is part of the SCC/CCR cluster. For information on how to configure cluster settings, see *Appendix A: Deploying PureMessage to Exchange clusters* (page 29).

11. In the **PureMessage Database settings** dialog box, specify the database (SQL server) where PureMessage will store reporting data, central quarantine, and policy configuration information. Click **Next**.

    PureMessage will automatically detect any local SQL database instances. If a local database instance is detected you choose it by selecting the **Local** option. If no database is detected and **Local** is chosen, then PureMessage will install a local instance of SQL Server Express. To use a database instance located on a different computer, choose the **Remote** option. The database **Browse** dialog displays only SQL server instances with the current domain.

    Note: For information on how to configure database mirroring, see *Appendix F: Database Mirroring* (page 43).

12. In the **PureMessage Service Credentials** dialog box, click **Create** and enter a password and confirm it to create a SophosPureMessage user. If the user account already exists, you will be prompted to enter its password. This account is used by Sophos PureMessage services. Click **Next**.
13. In the **PureMessage Configuration Group** dialog box, select a group you want to join or create a new group. Click **Next**.

    PureMessage installations can be grouped together to share the same policy configuration and be managed from a single management console. For more information, see *PureMessage Configuration Group* (page 11).

14. If you are installing PureMessage on an Exchange server that is configured as a mailbox-only role, the **PureMessage Mailbox Role Settings** dialog box is displayed. Select the Exchange transport server which PureMessage should use to send alert email messages. Click **Next**.
15. In the **PureMessage Administration Settings** dialog box, enter an Administrator email address. PureMessage will send alerts to this email address. You can change this address later too. Click **Next**.

    Note: PureMessage creates a security group in Active Directory called Sophos PureMessage Administrators, which includes all PureMessage administrators. By default, the current user will be added to this group.

16. In the **PureMessage Routing settings** dialog box, do as follows.

    a) Enter your company's email domain(s), such as mycompany.com, in the top panel.

    Note: You need not specify sub-domains. When you specify a domain, the sub-domains are included automatically.

    b) Enter the IP addresses of any trusted email relays, such as your ISP's SMTP server and any email gateway server or appliance upstream of your Exchange servers. Click **Next**.

    Note: PureMessage uses the upstream relays configuration to determine mail direction. Not configuring an upstream relay can cause PureMessage to classify mail from upstream relays as internal, and hence skip spam scanning for those messages. For information on configuring upstream (trusted) relays, see *Appendix B: How to configure upstream (trusted) relays* (page 36).

17. In the **Company Information** dialog box you can enter details relating to the size, location, and market sector of your company or organization. This valuable feedback helps SophosLabs analyse email security trends. Click **Next**.
18. In the **Start Copying Files** dialog box, ensure the settings are correct. If they are not, use the back button to return to previous dialog boxes and change the settings. When they are correct, click **Next**.
19. PureMessage displays the installation progress and installs Sophos Anti-Virus and Sophos AutoUpdate (if not already installed). Sophos AutoUpdate automatically downloads updates to virus data and anti-spam rules.

    Note: In certain circumstances the installation may require you to restart the server. The installation will continue after restarting.

20. When installation is complete, the InstallShield Wizard Complete dialog box is displayed. Click **Finish**.

If you also want to install a separate PureMessage administration console, see *Installing a PureMessage console on a separate computer* (page 10).

Note: If you have Microsoft Exchange server installed on your network, you may need to disable or exclude files from scanning. For more information see the Sophos support knowledgebase article *http://www.sophos.com/support/knowledgebase/article/40065.html*.

To start using PureMessage, see *Getting started with PureMessage* (page 13).

3.5 Installing a PureMessage console on a separate computer

The PureMessage administration console can be installed on a computer without the PureMessage service in order to manage remote PureMessage services.

To install PureMessage console onto a separate computer:

1. On the computer where you want to install the console, start the PureMessage installer.
2. In the **Welcome** dialog box, click **Next**.

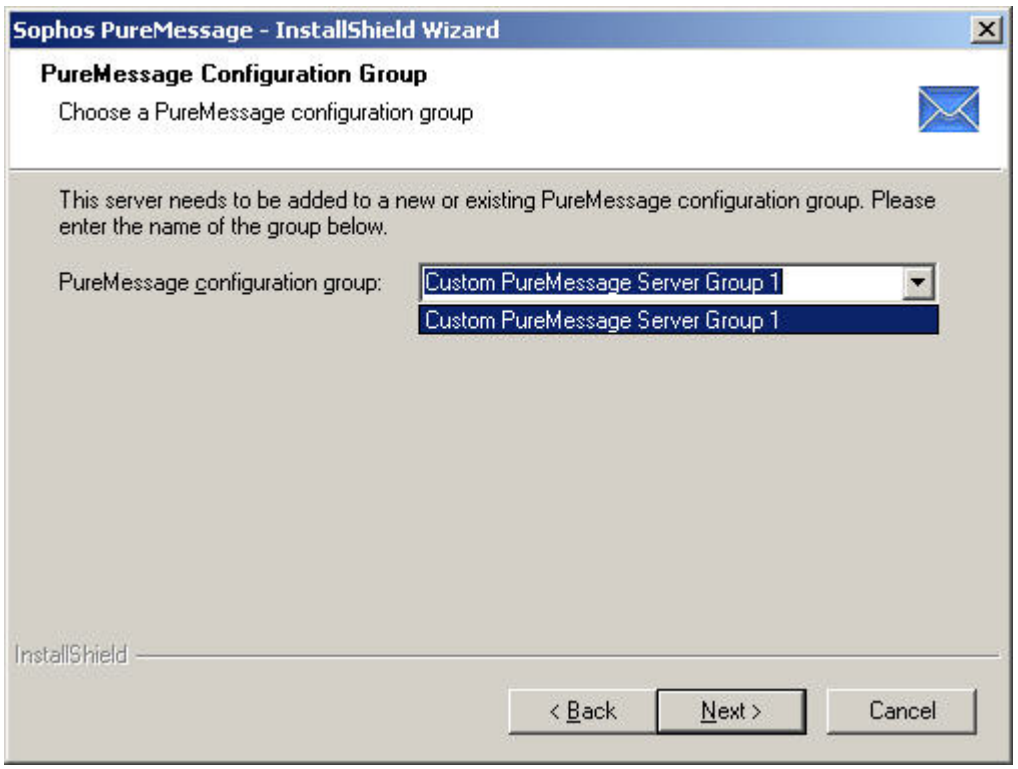
3. In the **License Agreement** dialog box, click **I accept** if you agree to the terms.
4. In the **Select Features** dialog box, clear the **PureMessage Service** check box and leave the **Administration Console** check box selected. Click **Next**.
5. In the **Choose Destination Location** dialog box, select your preferred destination folder, and click **Next**.
6. When installing in a Workgroup, the **PureMessage Service Credentials** dialog box will appear. Click **Create** and enter a password and confirm it to create a SophosPureMessage user. If the user account already exists, you will be prompted to enter its password. This account is used to connect to Sophos PureMessage services. Click **Next**.
7. In the **Start Copying Files** dialog box, click **Next**.
8. When installation is complete, the **InstallShield Wizard Complete** dialog box is displayed. Click **Finish**.
9. Double-click the PureMessage icon on your desktop to start the PureMessage administration console.

In certain circumstances the installation may require you to restart the server. The installation will continue after restarting.

3.6 PureMessage Configuration Group

If several PureMessage servers are required to implement the same policy then they should be installed to the same PureMessage group. This is achieved by selecting the same database and PureMessage group name during installation.

Once the first PureMessage server has been installed in a group, the group name becomes available from the **PureMessage Configuration Group** dialog box so that additional servers can be easily installed to the same group:


Sophos PureMessage - InstallShield Wizard
PureMessage Configuration Group
Choose a PureMessage configuration group
This server needs to be added to a new or existing PureMessage configuration group. Please enter the name of the group below.
PureMessage configuration group:
Custom PureMessage Server Group 1
Custom PureMessage Server Group 1
InstallShield
< Back
Next >
Cancel

All PureMessage servers in a group should be in the same Windows domain or Workgroup. If your Exchange 2007/2010 Edge servers are in a separate Workgroup then they should be managed separately.

For more information on installing PureMessage to an Exchange cluster, see *Appendix A: Deploying PureMessage to Exchange clusters* (page 29).

4 Starting and configuring PureMessage

This section tells you how to:

- Start PureMessage
- Configure PureMessage to acknowledge your mail domain and upstream trusted email relay (if not done during installation)
- Connect to your directory server.

4.1 Getting started with PureMessage

To start PureMessage, do as follows:

1. Double-click the **PureMessage** icon on your desktop.
2. In the PureMessage console, the left-hand pane (console tree) gives you access to the features you can configure. The right-hand pane (details) displays information or configuration options.

If you set up a mail domain and upstream email relay during installation, see *Connect to Active Directory* (page 14).

If you have not yet set up a mail domain, see *Set up a mail domain and upstream trusted relay* (page 13).

4.2 Set up a mail domain and upstream trusted relay

For PureMessage to determine inbound, outbound and internal mail correctly, you should configure your mail domains and any upstream (trusted) relays.

For information on configuring upstream (trusted) relays, see *Appendix B: How to configure upstream (trusted) relays* (page 36).

1. In the console tree, click **Configuration | System** and then click **Routing**.
2. In the **Routing** dialog box, do as follows:

   a) Click **Add**, and enter an address in the **Mail domains** panel, such as mycompany.com.

   Note: You need not specify sub-domains. When you specify a domain, the sub-domains are included automatically.

   b) To add an upstream trusted relay, click **Upstream (trusted) relays**.

3. In the **Upstream (trusted) relays** dialog box, click **Add** to specify an upstream trusted relay address or range of addresses.
4. In the **Specify Host IP Addresses** dialog box, enter a single IP address or a range of addresses. You can also enter a comment for administrative use and click **OK**.
5. In the **Upstream (trusted) relays** dialog box, click **OK** to save your relay(s).
6. In the **Manage changes** menu, click **Save changes**.

PureMessage now recognizes your specified mail domains and upstream (trusted) relays.

Now connect to Active Directory. See *Connect to Active Directory* (page 14).

4.3 Connect to Active Directory

You can configure PureMessage to integrate with Microsoft Active Directory. You can then use recipient validation features and create message policies based on users and groups already configured in the directory server. If you do not need to use these features, skip this section.

Note: To configure directory server settings when using ADAM/AD LDS, see the *PureMessage for Microsoft Exchange user manual*.

1. In the console tree, click **Configuration | Users and groups** and click **Active Directory**.
2. In the **Active Directory** dialog box, click **Detect Active Directory**. The directory server settings should be filled in automatically. If not, you may need to fill in the directory server settings manually.
3. Enter the user name and password in the Logon Credentials pane if you are synchronizing with an instance of ADAM/AD LDS or if you are synchronizing with the Active Directory Global Catalog Server. Otherwise, PureMessage will log on using the SophosPureMessage service account.
4. Click **Verify settings**. PureMessage will attempt to log on to your directory server.

5. Ensure the **Synchronize with Active Directory checkbox** is checked. You can then configure PureMessage to synchronize with Active Directory (refresh its local copy) automatically or periodically.

   PureMessage keeps a local copy (cache) of the users and groups from Active Directory for performance reasons.

6. Click **Synchronize now** to start the synchronization process instantly.

If you have selected **Automatic synchronization** and if a change is made to an entity in Active Directory, it may take about 15 minutes for the change to reflect in PureMessage.

Before you can set up your transport (SMTP) and Exchange store configuration, you need to set up alerts. See *Setting up alerts* (page 16).

5 Setting up alerts

In order to receive PureMessage administrator alerts, you must configure this feature. You can also set up a template for alerts.

5.1 Setting up an address for alerts

1. In the console tree, click **Configuration | System** and then click **Alert configuration**.
2. In the **Email addresses** tab of the **Alert configuration** dialog box, click **Add**. Enter the administrator's email address in the **Send administrator alerts to** panel.
3. Enter an email address in the **Sender email address** panel. The email address will be used for sending out alerts and other PureMessage-generated messages.
4. Click **OK** to save your changes.

5.2 Setting up a template for email alerts

The default email template for alerts is sufficient for some users' needs. However, you can customize the template as described below.

1. In the console tree, click **Configuration | System | Alert configuration** and then click the **Alert template** tab.
2. In the **Alert subject** panel, enter the subject line of the alert. Right-click in the edit panel to view available substitution symbols.

   Substitution symbols can insert variables such as date or other information specific to the message.

3. In the **Alert body text** panel, create the main body of your alert. Right-click within the text field to view substitution symbols.
4. In the **Text for each incident** panel, enter any unique per-incident text you want to display.
5. In the **Alert Templates** tab, click **OK**.
6. In the **Manage changes** menu, click **Save changes**.

PureMessage alerting is now configured.

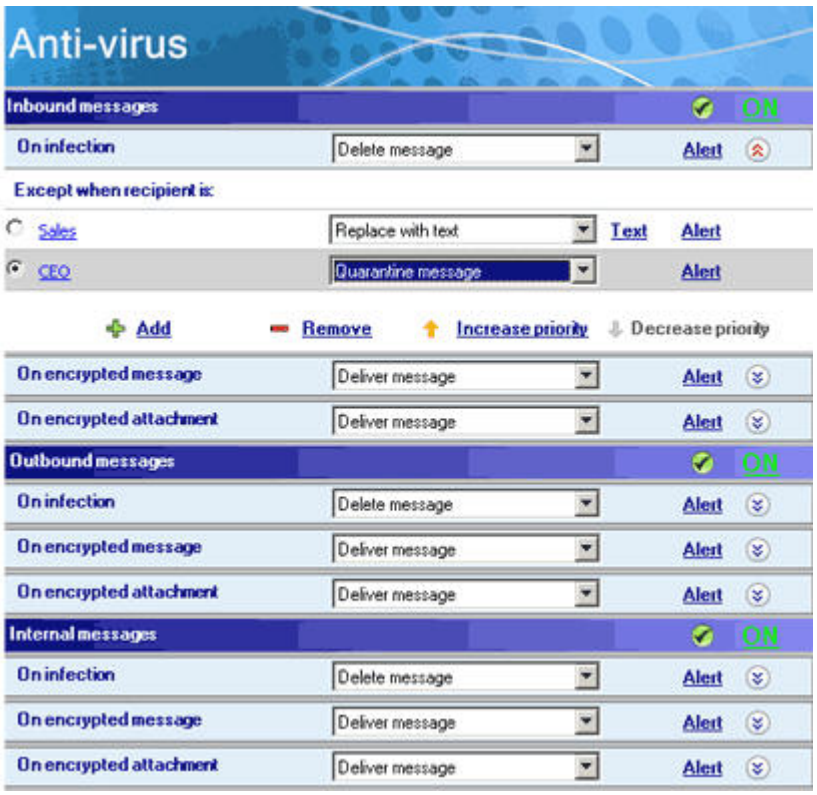
Now see *Ensuring anti-virus scanning is enabled* (page 17).

6 Ensuring anti-virus scanning is enabled

By default, anti-virus scanning is enabled for inbound, outbound, and internal mail.

To check that anti-virus scanning is enabled, follow these steps:

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy** and then click **Anti-virus**.
2. In the **Anti-virus** screen, ensure that the scanning status icons in the inbound, outbound, and internal message title bars are Green, and display **ON**.



Note: You can define separate policies for each direction of mail, and you can define specific policies for exempt users and groups. For more information, see the *PureMessage for Microsoft Exchange user manual.*

PureMessage now protects against viral threats.

Next, see *Blocking files which may contain threats* (page 18).

7 Blocking files which may contain threats

Sophos recommends that you block inbound email attachments that are most likely to contain threats.

The **On suspicious attachment policy** rule is preconfigured to block file types that are commonly used to transport email threats, such as executable files (.exe, .scr, .com, .pif, etc). By default this rule is turned off.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy** and then click **Content**.
2. In the **Content filtering** screen, ensure the status icon for inbound mail title bar is Green and displays **ON**.
3. Select the **On suspicious attachment** checkbox. Click **Define** to view and edit file types predefined by Sophos as suspicious attachments.
4. In the **Inbound messages - Suspicious attachment type** dialog box, click the **Attachment types** tab.
5. In the **Attachment types** tab, the attachment types in the **Executable** and **Object Code** groups are selected by default. On the **Attachment names** tab the **Block multiple extensions** option is selected by default.
6. Check the **Block potentially unwanted applications (PUAs) except** checkbox.
7. If you wish to allow users access to otherwise blocked applications, click **Add** to enter a PUA that you want to allow. PUA names can be found at *http://www.sophos.com/security/analyses/*.
8. Click **OK** to save your changes and return to the **Content filtering** pane.
9. In the **Content filtering** dialog box, under the **Inbound messages** bar, in the **On suspicious attachment** panel, select **Quarantine message** from the drop-down menu.
10. Under the **Inbound messages** bar, in the **On suspicious attachment** panel, click **Alert**.
11. In the **Alert configuration** dialog box, check one or more checkboxes to specify who will be notified in the event of PureMessage quarantining a suspicious attachment. Click **OK** to save your changes and return to the **Content filtering** pane.
12. In the **Manage changes** menu, click **Save changes**.

    Note: For information on configuring the content settings of your policy, see the *PureMessage for Microsoft Exchange user manual*.

PureMessage now

- blocks and quarantines inbound messages with suspicious attachments.
- sends alerts to those you specified.

Now you can enable spam blocking, scan the Exchange message store, and tell users about quarantined mail. These functions are described in the sections that follow.

8 Blocking spam

You can configure PureMessage to deal with spam (unwanted incoming email). A typical anti-spam setting would be to delete spam and quarantine suspected spam.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy** and then **Anti-spam**.
2. In the **Anti-spam** screen, in the **Inbound messages** bar, ensure the ON/OFF icon displays **ON**. If it displays **OFF**, click the icon to turn it on.
3. In the **On-spam** panel, select **Delete message** (or your preferred setting) from the drop-down menu.
4. In the **On suspected spam** panel, select **Quarantine message** (or your preferred setting) from the drop-down menu.
5. In the **Manage changes** menu, click **Save changes**.

Next you specify which mails you will categorise as spam and suspected spam by setting the spam ratings for PureMessage.

8.1 Change anti-spam settings

PureMessage gives each email a spam rating. The higher the rating, the more likely the email is to be spam. PureMessage uses this rating to decide whether the email should be treated as spam or suspected spam.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy | Anti-spam** and then **Change anti-spam settings**.
2. In the **Anti-spam settings** dialog box, use the slider controls to adjust the threshold, above which PureMessage regards an email as spam or suspected spam.

   Note: Sophos recommends you set your ratings above 50 to avoid legitimate mail being classed as spam or suspected spam.

3. Ensure the **Check reputation of message relays against external DNS block lists** checkbox is checked. Enabling this option will check incoming messages against the IP addresses of known spam sources and will filter out any messages coming from these IP addresses.
4. In the **Anti-spam settings** dialog box, you can check the **Check reputation of first external relay only** checkbox only after configuring upstream (trusted) relays correctly. This option will only check the first external relay, for more deterministic spam scoring.
5. If you want to add the spam score as a SCL rating, check the **Add spam score to message as Microsoft Spam Confidence Level (SCL) rating** checkbox. Messages delivered to end users with a SCL rating higher than a particular value are diverted into the user's Junk mail folder in Microsoft Outlook. Click **OK** to save your changes.
6. In the **Manage changes** menu, click **Save changes**.

For optimal spam detection, ensure PureMessage has up-to-date information regarding the addresses of any upstream (trusted) relays. For more information on configuring the anti-spam settings of your policy, see the *PureMessage for Microsoft Exchange user manual*.

9 Scanning Exchange Message Stores

You can configure PureMessage to scan both private and public Exchange stores.

- On-access scanning is done in real-time when new items are added to the Exchange Store and accessed by an email client.
- Proactive scanning occurs when messages and files are written to the Information store.
- Background scanning is done continuously at off-peak times.

For more information, see *Exchange Store scanning* (page 39).

9.1 Enable store scanning and alerts

1. In the console tree, click **Configuration | Exchange store scanning policy**.
2. In the **Anti-virus** dialog box, in the **Exchange store scanning** panel, ensure the ON/OFF icon displays **ON**. If it displays **OFF**, click the icon to turn it on.
3. In the **On infection** panel, select "Replace attachment with text" from the drop down menu. The **Text** button appears. If you click the **Text** button, you can edit the text shown when PureMessage replaces an infected attachment.
4. In the **On infection** panel, click **Alert**.
5. In the **Alert configuration** dialog box, ensure the **Administrator** checkbox is checked and click **OK** to save your changes and return to the **Anti-virus** (**Exchange store scanning**) pane.
6. In the **Manage changes** menu, click **Save changes**.

PureMessage now

- scans the Exchange information store for viruses, and replaces the attachment with the configured text.
- sends an alert to the Administrator.

Now configure scanning of Exchange stores.

9.2 Configure scanning of Exchange stores

Note: The Exchange Store is made up of both public and private stores.

- A public store is a database that is accessible to multiple users.
- A private store (example, a mailbox) is usually only accessible to a single user.

1. In the console tree, click **Configuration | Exchange store scanning policy** and then click **Change exchange store scan settings**.
2. In the **Exchange store scan settings** dialog box, select the **Stores** tab.

3. In the **Stores** tab, in the **Exchange private store** panel, choose the appropriate checkboxes to enable on-access, proactive, and/or background scanning in the private store.
4. In the **Exchange public store** panel, choose the appropriate checkboxes to enable on-access, proactive, and/or background scanning in the public store.
5. If you want background scanning to be enabled only outside office hours, then check the **Enable background scanning only for out of working hours** checkbox, and select your working days and times.
6. Click **OK** to save your changes.
7. In the **Manage Changes** menu, click **Save changes**.

PureMessage now scans items as configured by your settings.

10 Dealing with quarantined items

Depending on your configuration, PureMessage can quarantine mail that:

- is infected.
- is spam, or suspected spam.
- is encrypted, or has an encrypted attachment.
- has a suspicious or unwanted attachment.
- contains a blocked phrase or offensive language.
- is unscannable, or creates a scanning error.

Quarantined messages are isolated in a secured format in a central location on disk. Administrators can deal with these messages in a number of ways, such as disinfect, delete, or deliver them.

You can also enable users to access a spam quarantine website, where they can review and deal with their quarantined spam messages.

This section tells you how to:

- do quarantine database housekeeping.
- deal with quarantined messages.
- enable end-users to access the spam quarantine website.
- set up digests to tell users about spam and suspected spam.

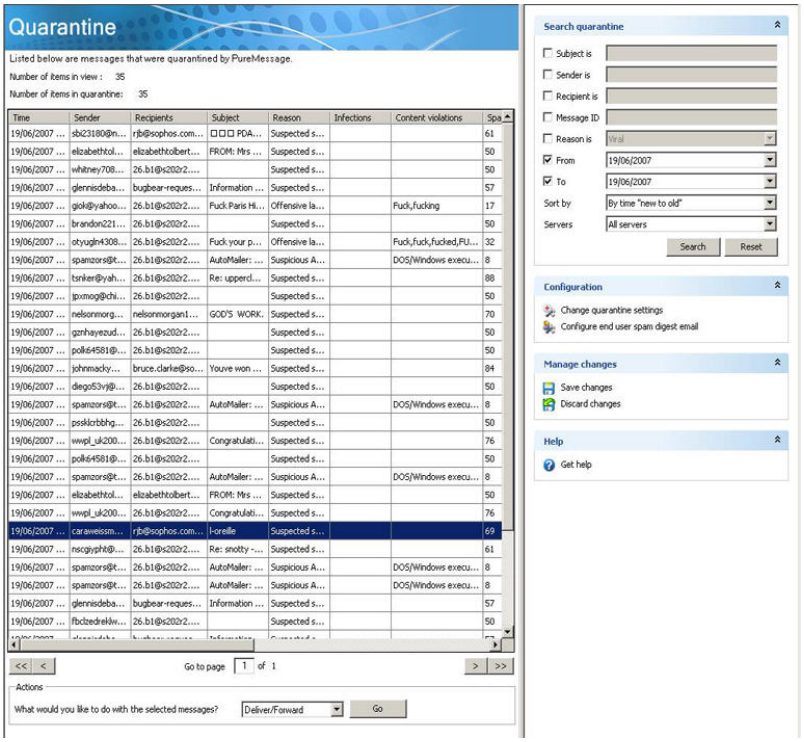
10.1 Quarantine housekeeping

You can specify the number of days to keep quarantined mail before deleting it.

1. In the console tree, click **Quarantine**.
2. In the **Configuration** menu, click **Change quarantine settings**.
3. In the **Quarantine settings** dialog box, specify the number of days you want to keep quarantined mail before deleting it in the **Number of days to keep mails in quarantine before deletion** box.
4. Click **OK** to save your settings, and return to the **Quarantine** pane.
5. In the **Manage Changes** menu, click **Save changes**.

10.2 Dealing with quarantined messages

1. In the console tree, click **Quarantine**.



   From this pane, you can enter search criteria in the **Search** panel, searching on subject, sender, recipient, message ID, reason for quarantine, or any combination of these. You can also filter your search by date using the **To** and **From** fields.

2. The list of quarantined messages is displayed in the details pane. Double-click an item for more details such as reasons for quarantining.
3. To deal with an item, highlight it, select an action from the drop-down menu in the **Actions** pane, and then click **Go**. You can delete a quarantined item or, remove the virus(es) and deliver it. If you believe mail to be wrongly classified please submit the item to Sophos for analysis. If you selected **Deliver/Forward**, go to step 4, otherwise the selected action is performed.
4. If you choose **Deliver/Forward** from the drop-down **Actions** menu, the **Deliver message(s)** dialog box appears. In the **Deliver messages** dialog box you can deliver the selected message(s) to intended recipients or to specified recipients. You can use this feature to forward quarantined items to an administrator to review the content of the email.

   For more information, see the *PureMessage for Microsoft Exchange user manual*.

5. Note that PureMessage delivers a copy of the email. The original file remains in the quarantine folder for the number of days specified in the **Quarantine settings** dialog box, unless you choose to **Automatically delete message(s) from quarantine after delivery**.
6. If you want to add the sender to your list of trusted senders, check the **Add sender to allowed list (skip spam scanning for this sender)** checkbox.
7. Click **OK** to save your changes.

10.3 Enabling end-users to access the spam quarantine website

There are two ways to enable end-users access the spam quarantine website.

You can set a task to send all users with quarantined spam mail an email notification, so they can click a link to access the website. See *Setting up quarantine digest emails to users* (page 25).

Alternatively, if you use Active Directory, users can visit the spam quarantine website directly at any time using a web browser such as Internet Explorer, at the following address:

```
http://servername:port/
```

Where `servername` is the name of the server on which PureMessage is installed and `port` is the port number for the quarantine digest website (port 8081 by default).

When the user accesses the website, Internet Information Services (IIS) will authenticate the user with Windows Authentication. If the user owns multiple email addresses (aliases), the spam quarantine website will show email messages quarantined for all the addresses.

If you want to distribute written instructions to your users that explain how to access the spam quarantine website, see the *PureMessage for Microsoft Exchange user manual*.

10.4 Setting up quarantine digest emails to users

PureMessage can send each user a message informing them that some of their email has been quarantined as spam. The user can follow a link to the web-based spam quarantine where they can delete unwanted mail, or retrieve wanted mail. To do this, set up spam quarantine digest email and schedule times when PureMessage should send it out.

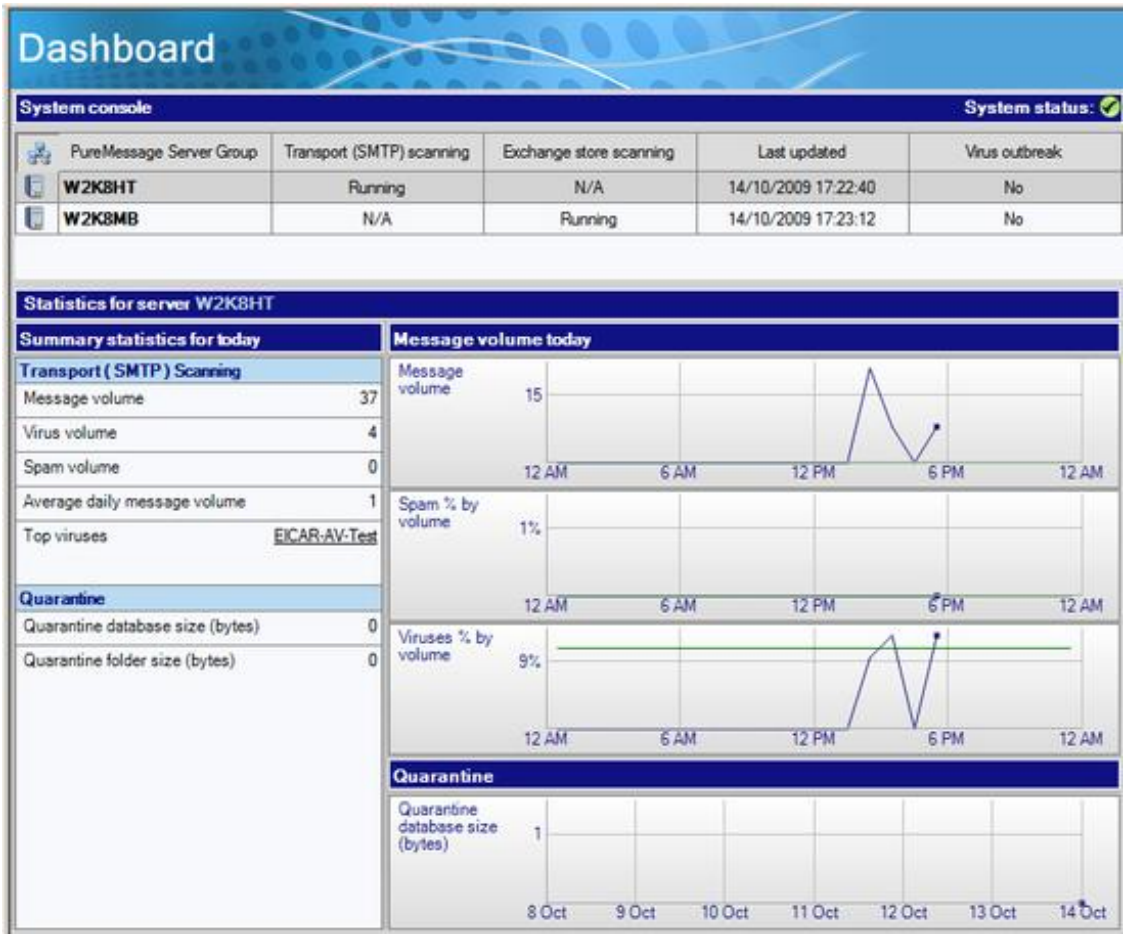
1. In the console tree, click **Configuration | Users and groups** and click **End user spam digest email**.
2. In the **End user spam digest email** dialog box, enter a subject in the **Digest subject** text box.
3. In the **Digest body text** panel, edit the digest as appropriate, or accept the default text. To enter or edit a substitution symbol, right-click and select a substitution symbol from the drop-down menu.
4. In the **Send digests on** panel, select the days and times you want to send out digests. Click **OK** to save your changes.
5. In the **Manage Changes** menu, click **Save changes**.

PureMessage now sends quarantine digest emails to users at specific times.

11 Monitoring system activity

The dashboard shows the system status and displays current statistics that provide the information about the health of all the servers on the system.

In the console tree, click **Dashboard**.



By default, the servers are listed in alphabetical order on the dashboard, unless one or more registers a system failure. In this case, the System Status traffic light becomes red, the faulty server is marked with a warning icon, and the server is displayed at the top of the list.

For each server, the **System console** panel displays the following information:

- Whether Transport (SMTP) Scanning is Running, Stopped (by user), or Unavailable. If the status is unavailable, an alert is displayed.
- Whether Exchange Store scanning is Running, Stopped (by user), or Unavailable. If the status is unavailable, an alert is displayed.

- Whether the last update succeeded, and if so, the time and date it took place. If it did not succeed, an alert is displayed.
- Whether there is a virus outbreak, and if so, on which server.
- For the selected server, the **Summary statistics for today** panel displays scanning and quarantine information for today (that is, since midnight) and shows the trends for each main category of information in the form of a graph. The information includes:
  - The current day's transport (SMTP) scanning statistics (including message volume, spam and viruses).
  - The current day's Exchange store scanning statistics (including attachments processed, and viruses detected).
  - The current day's quarantine statistics.

All information is refreshed every two minutes.

12 Uninstalling PureMessage

On Exchange 2007/2010, PureMessage should be uninstalled from the mailbox-only role before it is uninstalled from the Exchange transport server. To uninstall PureMessage, do as follows:

1. If the PureMessage Administration console is open on any server, close it.
2. At the taskbar, click **Start | Settings | Control Panel**.
3. In **Control Panel**, double-click **Add/Remove Programs**.
4. In the **Add/Remove Programs** dialog box, select **Sophos PureMessage** and click **Remove**.
5. In the **Confirm Uninstall** message box, click **Yes**.

   A progress bar is displayed. Wait for uninstallation to complete.

13 Appendix A: Deploying PureMessage to Exchange clusters

13.1 How PureMessage works with Exchange clusters

PureMessage incorporates a cluster-aware service that can be installed across multiple nodes. This allows PureMessage to be used with clustered Microsoft Exchange servers and to take advantage of the increased resilience that a cluster offers.

Clustered systems are inherently more complicated than non-clustered systems and we recommend that you read the whole of this section before starting to install PureMessage on a cluster.

If you still have questions about installing PureMessage on a cluster after reading this section, contact Sophos technical support.

13.2 Before you install

13.2.1 Database requirements

For cluster server installations, PureMessage cannot use a local MSDE or SQL Server Express instance. Alternatively, you may connect to any one of the following:

- A local clustered virtual SQL Server instance
- A remote SQL Server instance
- A remote MSDE or SQL Server Express instance

You must install SQL Server, SQL Server Express, or MSDE before installing PureMessage. Microsoft SQL Server is not distributed with PureMessage.

If you are currently using MSDE or SQL Server 2000 database, it is recommended that you upgrade to SQL Server 2005 or later (any edition) for optimized performance.

For details on how to upgrade existing MSDE or SQL Server 2000 database, see *http://www.sophos.com/support/knowledgebase/article/31157.html*.

13.2.2 Installation requirements

When installing PureMessage on nodes in a cluster, make sure that you meet the following requirements:

- The path to the installation folder must be identical on each node.
- The IIS websites present on each node of the cluster must be identical. In particular, the allocated port numbers of each site must be the same across nodes.

- For Cluster Continuous Replication (CCR), a clustered Microsoft Exchange 2007 system must be configured to operate in CCR mode.
- For Single Copy Cluster (SCC), a clustered Microsoft Exchange 2003 or 2007 system must be configured to operate in SCC mode.
- For SCC, a shared drive is required for storing files that are to be shared between cluster nodes. The shared drive must have a disk resource present in the same cluster group as the Exchange cluster resources.

For SCC/CCR clusters, ensure your cluster type is supported:

Cluster type	Supported?	Document type
Active/Passive	Yes	PureMessage is supported on all Active/Passive clusters regardless of how many active or passive nodes are present within the cluster. This includes popular cluster configurations such as A/P, A/A/P and A/A/A/P.
Active/Active	No	Since an Active/Active cluster could require multiple instances of PureMessage to be online on a single node at a particular time, this type of cluster is not supported.

13.3 Important information about installing on CCR and DAGs

For Cluster Continuous Replication (CCR) and Database Availability Groups (DAGs), PureMessage uses DFS Replication (DFSR) to copy quarantine files between nodes.

- If you are joined to a Windows Server 2000 or Windows Server 2003 non-R2 domain, DFSR requires that object classes be added to the domain directory partition to contain replication groups and content sets before installing PureMessage.

  Read *http://www.sophos.com/support/knowledgebase/article/57333.html* to learn how to do this.
- If you are installing PureMessage on a Windows Server 2008 computer that is running SP1 and is joined to a pre-Windows Server 2008-based domain, read *http://www.sophos.com/support/knowledgebase/article/57334.html* before you begin.

13.4 Installation procedure on CCR

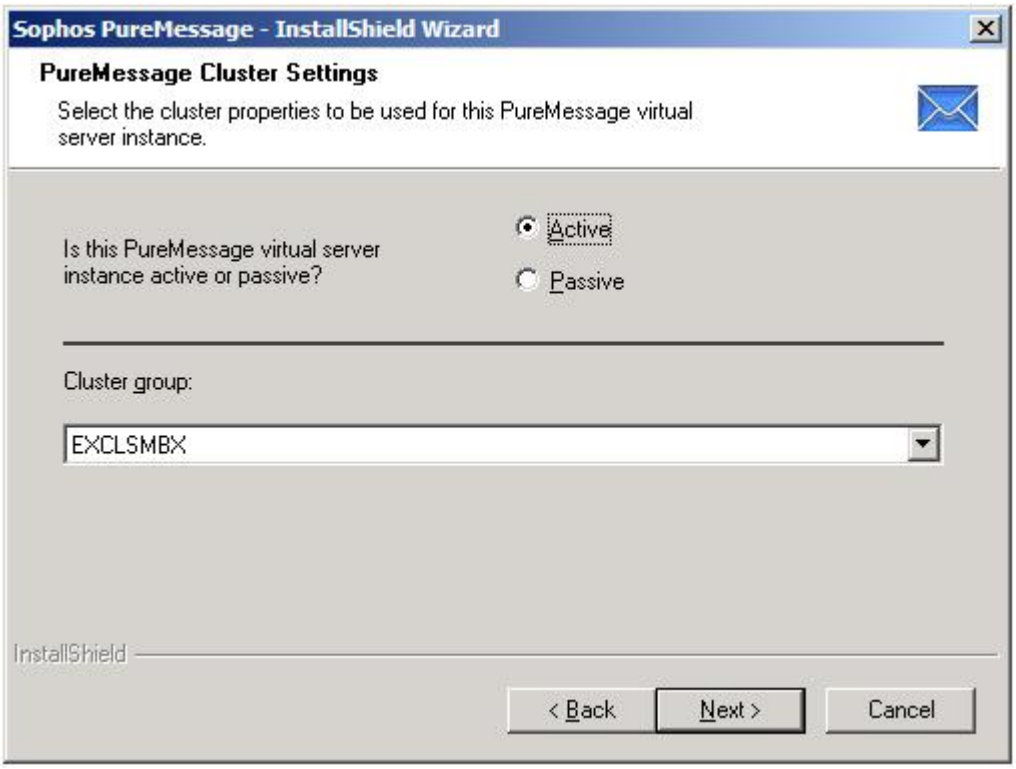
- Do not install on different nodes within a cluster concurrently. The PureMessage service should be installed on each node within the cluster one after another, but not simultaneously.
- Installations must be performed on both the active and passive nodes.
- You should not failover or move cluster groups during the installation process.

In order to meet these installation criteria, the following installation procedure is recommended:

- Run the PureMessage installer and let the InstallShield Wizard guide you through installation, as described in *Installing PureMessage* (page 6).

  Information about an additional screen that will appear is provided below.

  - When installing PureMessage on each active node that owns an Exchange virtual server instance. On the **PureMessage Cluster Settings** dialog, select **Active** for the PureMessage virtual server instance and choose the corresponding **Cluster Group** from the drop-down menu.
  - When installing PureMessage on each passive cluster node. On the **PureMessage Cluster Settings** dialog, select **Passive**.



13.5 Installation procedure on DAGs

Database Availability Groups (DAGs) are used for implementing high availability in Exchange 2010.

- Do not install on different DAG members concurrently. The PureMessage service should be installed on each DAG member one after another, but not simultaneously.

- If a DAG member has PureMessage installed and if it is added or removed from the DAG, then PureMessage must be reinstalled on that server. This is required so that the replication settings on the server are updated.

  To maintain Exchange availability during the re-install of PureMessage, the mailbox databases hosted on the server should be moved to an alternative server in the DAG.

13.6 Installing PureMessage on an Exchange SCC

- Do not install PureMessage on different nodes within a cluster concurrently. The PureMessage service should be installed on each node within the cluster one after another, but not simultaneously.
- Installations must be performed on each active node hosting an Exchange virtual server instance and on each passive node.
- You should not failover or move cluster groups during the installation process.

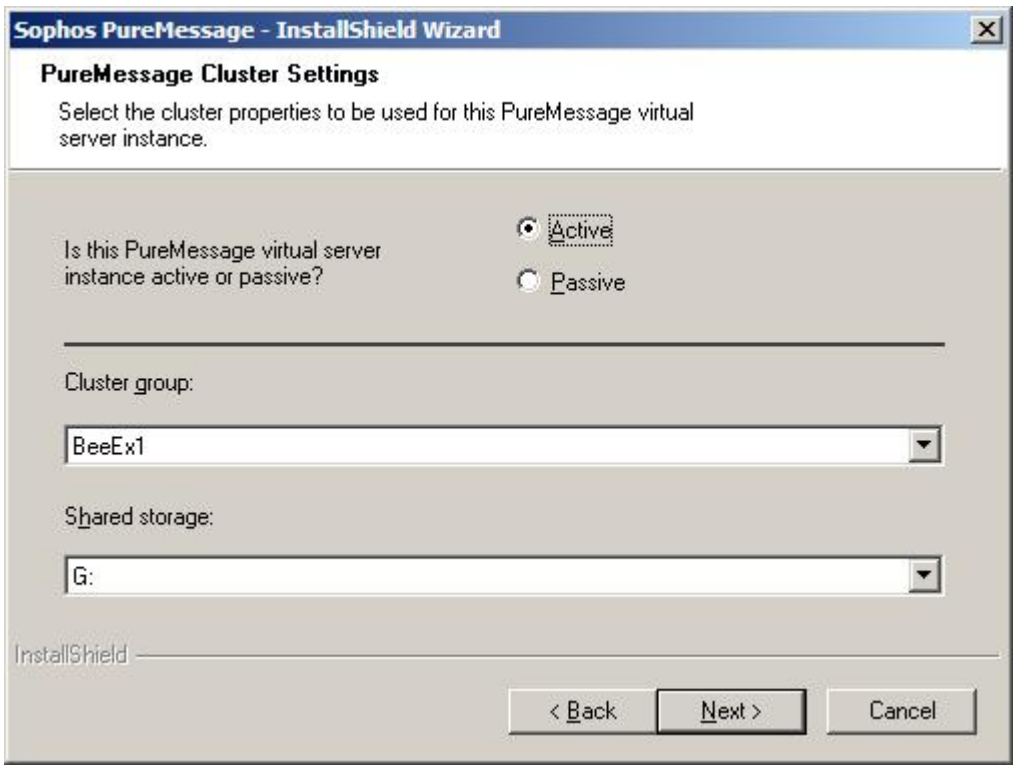
In order to meet these installation criteria, the following installation procedure is recommended:

1. Ensure that each Exchange virtual server instance is owned by a different cluster node. This is the normal arrangement for an operational Exchange cluster so will usually require no action.
2. Run the PureMessage installer and let the InstallShield Wizard guide you through installation, as described in *Installing PureMessage* (page 8).
3. Install PureMessage on each cluster node one after another, but not simultaneously, owning an Exchange virtual server instance (active node).

   On the **PureMessage Cluster Settings** dialog, select **Active** and then choose the **Cluster group** and **Shared storage** corresponding to the owned Exchange virtual server instance. The shared storage is used for sharing PureMessage files across the nodes.

4. After installation on all active nodes, install PureMessage, one after another, but not simultaneous on each remaining passive cluster nodes.

   When installing on the passive node, on the **PureMessage Cluster Settings** dialog, select **Passive**.



13.6.1 Example: Two-node (A/P) cluster

A two-node A/P is the simplest type of cluster that PureMessage can be installed on.

1. Install the PureMessage service on the node that owns the Exchange virtual server instance.

   On the **PureMessage Cluster Settings** dialog, select **Active** and then choose the **Cluster group** and **Shared storage** corresponding to the owned Exchange virtual server instance.

2. Repeat the installation for the other passive node.

   On the **PureMessage Cluster Settings** dialog, select **Passive**.

13.6.2 Example: Four-node (A/A/A/P) cluster

An A/A/A/P cluster has four nodes (three active and one passive) and three Exchange virtual server instances (one on each active node).

1. Make sure that the three Exchange virtual server instances are owned by three different nodes. This is the normal arrangement for an operational Exchange cluster so will usually require no action.

2. Install the PureMessage service on the first active node using settings appropriate for the first Exchange virtual server instance.

   On the **PureMessage Cluster Settings** dialog, select **Active** and then choose the **Cluster group** and **Shared storage** corresponding to the owned Exchange virtual server instance.

3. Install the PureMessage service on the second active node using settings appropriate for the second Exchange virtual server instance.

   On the **PureMessage Cluster Settings** dialog, select **Active** and then choose the **Cluster group** and **Shared storage** corresponding to the owned Exchange virtual server instance.

4. Install the PureMessage service on the final active node using settings appropriate for the final Exchange virtual server instance.

   On the **PureMessage Cluster Settings** dialog, select **Active** and then choose the **Cluster group** and **Shared storage** corresponding to the owned Exchange virtual server instance.

5. Install the PureMessage service on the passive node.

   On the **PureMessage Cluster Settings** dialog, select **Passive**.

13.7 Uninstalling PureMessage from a cluster

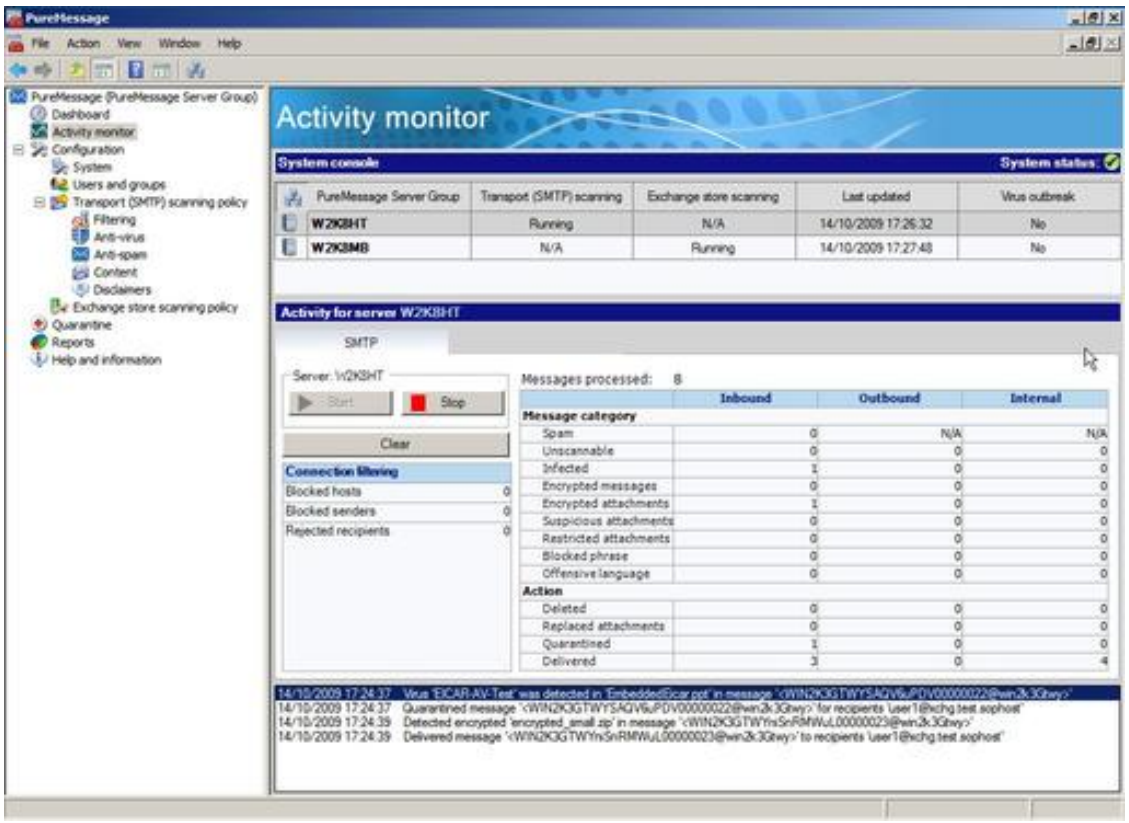
All PureMessage administration consoles (if running) need to be closed from all servers before uninstalltion. Follow instructions in *Uninstalling PureMessage* (page 28).

13.8 Administering PureMessage on a cluster

Several PureMessage servers may be arranged into a group and administered together from a single PureMessage console. All PureMessage servers in a group have the same policy settings applied to them, that is, when a policy change is made it is automatically applied to all the servers in the group.

13.8.1 Using the PureMessage administration console

In order to manage a group of PureMessage servers, the PureMessage console should connect to any server in the group. When policy changes are made, they will be automatically applied to all services in the group. Additionally, the activity monitor and dashboard screens will display status information for all the servers in the group:



In order to manage a different group of PureMessage servers from the same console, it is necessary to disconnect from the current group and reconnect to a server from the new group.

To do this, on the PureMessage toolbar, click on the **Select server** icon.

14 Appendix B: How to configure upstream (trusted) relays

You should configure any upstream (trusted) relays to improve your email scanning speed and spam detection.

By default, PureMessage will run a reputation check on each email server address specified in an email. When a server is added to the upstream (trusted) relay list, the reputation check for that server is skipped. Because a lower volume of reputation checks has to be carried out, this improves the email scanning speed.

Upstream (trusted) relays also enable the spam engine to match an email server's address against the known list of spamming email servers with more precision. A higher spam score can therefore be allocated to the email when a match is found.

14.1 Which upstream relays should be defined as trusted?

You should define as an upstream (trusted) relay any email relay that sends or forward emails to PureMessage and that meets one of the following criteria (as in Figure 3):

- Your ISP's SMTP server.
- Any email relays located on your network which are upstream to your PureMessage server(s).
- A server which delivers mail to other servers in a cluster.

For more information see, *Set up a mail domain and upstream trusted relay* (page 13).

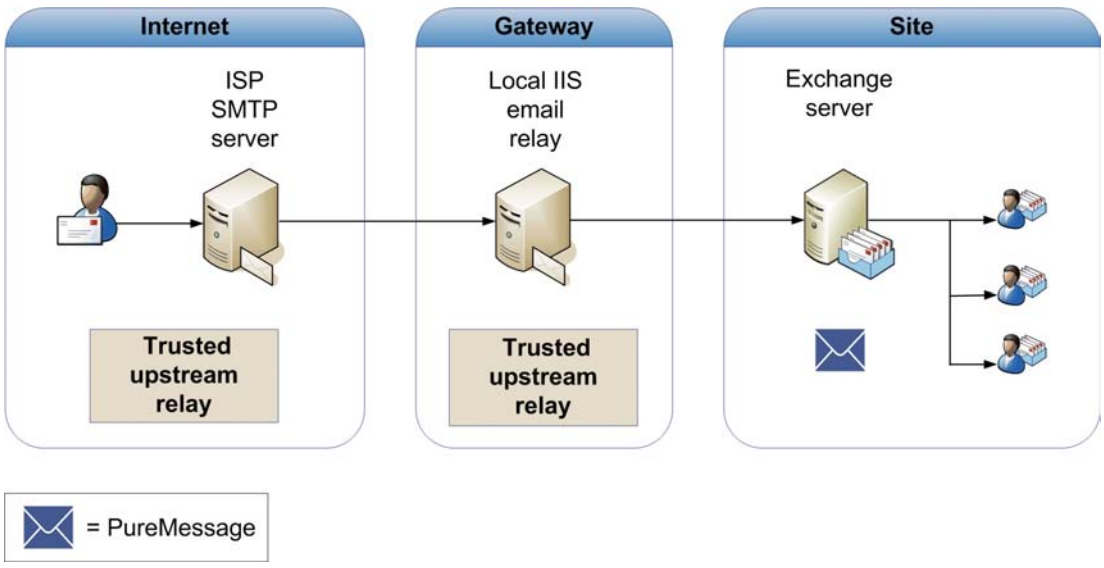


Figure 3: Trusted upstream relays

15 Appendix C: How does PureMessage route mail?

PureMessage uses the configured mail domains, trusted upstream relays, and IP address of the connecting host to distinguish between inbound, outbound and internal mail.

1. Is the recipient domain on the configured mail domain list?

   No: the message is *outbound*.

   Yes: go to step 2.

2. Is the sender's IP address external?

   Yes: the message is *inbound*.

   No: go to step 3.

3. Is the sender's IP address internal or unavailable?

   Internal: go to step 4.

   Unavailable: the message is *internal*.

4. Is the internal IP address on the list of trusted relays?

   Yes: the message is *inbound*.

   No: the message is *internal*.

16 Appendix D: About PureMessage mail scanning

PureMessage scans all SMTP inbound, outbound, and internal email messages and Exchange store emails and includes threat reduction technology to protect against new or unknown email-borne threats.

16.1 SMTP scanning

16.1.1 SMTP filtering

The SMTP filtering options in PureMessage perform recipient validation and use custom block lists to block hosts and messages in order to reduce the processing overhead on the server and save bandwidth.

Recipient validation

Organisations receive a lot of spam messages that are addressed to non-existent users. Recipient validation allows you to discard messages addressed to non-existent users.

This option requires a connection to a directory server or custom users and groups to provide the email addresses which are used to validate recipients. Typically this will be an Active Directory server.

Block lists

Block lists allow you to specify hosts and senders from whom PureMessage should not accept any messages.

Note: For information on enabling recipient validation and creating block lists, see the *PureMessage for Microsoft Exchange user manual*.

16.1.2 Anti-virus policies

You can define separate anti-virus policies for inbound, outbound and internal mail.

For information on configuring anti-virus scanning, see *Ensuring anti-virus scanning is enabled* (page 17).

16.1.3 Anti-spam policy

If your license permits, you can define an anti-spam policy.

PureMessage applies the anti-spam policy only to inbound messages. The anti-spam policy is On by default and applies to all users, but you can configure exceptions.

For information on defining an anti-spam policy, see *Blocking spam* (page 19).

16.1.4 Content filtering policies

PureMessage scans inbound, outbound and internal mail and filters unwanted content such as administrator-defined phrases and offensive language. You can define policies to filter content in a message header, subject, body, and/or attachment.

Note: For information on defining content filtering policies, see *Appendix E: Filtering attachments containing unwanted content* (page 41).

16.1.5 Attachment blocking

PureMessage can block suspicious or unwanted attachments and PUAs according to user-defined attachment types.

For information on blocking attachments and PUAs, see *Blocking files which may contain threats* (page 18).

16.2 Exchange Store scanning

PureMessage provides on-access, proactive, and background scanning of Exchange private and public information stores using the Microsoft Virus Scanning API (VSAPI).

Each time an item is scanned, it is stamped with an ID which indicates the virus signature version number at the time of scanning. An item will be rescanned *only* if a more up-to-date virus signature has been released by Sophos.

For more information on VSAPI, see the Microsoft Knowledge Base article *http://support.microsoft.com/kb/285667/en-us*.

16.2.1 On-access scanning

When on-access scanning is enabled, new items in the Exchange Store are scanned as soon as they are accessed by a client such as Microsoft Outlook.

On-access scanning is **enabled** by default for both private and public information stores.

For information on enabling on-access scanning, see *Configure scanning of Exchange stores* (page 21).

16.2.2 Proactive scanning

When proactive scanning is enabled, new items submitted to the Exchange Store are added to a queue for scanning by Exchange server.

Exchange server assigns each new item a low priority in the queue, so that they do not interfere with the scanning of high-priority items. Exchange server automatically upgrades their priority, if a client attempts to access them while they are in the low-priority queue.

Proactive scanning is enabled by default for both private and public information stores.

For information on enabling proactive scanning, see *Configure scanning of Exchange stores* (page 21).

16.2.3 Background scanning

Exchange server background scanning continuously navigates the entire Exchange Store. As items that have not been scanned are encountered, they are submitted to PureMessage for scanning.

Background scanning is **disabled** by default for both private and public information stores.

As background scanning has a performance impact on the Exchange server, we recommend that you schedule it to run during periods of low server activity. Background scanning schedules can be defined in the Exchange store scan settings dialog.

Note: The scanning process will be reset if a virus signature update is received from Sophos. For large message stores, this can mean that background scanning will not complete a full scan of the store.

For information on defining background scanning periods and enabling background scanning, see *Configure scanning of Exchange stores* (page 21).

17 Appendix E: Filtering attachments containing unwanted content

PureMessage can analyse content within common document types. This enables you to search for phrases within those documents when they are attached to messages as files and apply policy rules accordingly.

PureMessage can extract content from the following file types:

- Plain text (TXT)
- HTML
- Rich text (RTF)
- PDF
- Microsoft Office documents (DOC, DOCX, PPT, PPTX, XLS, XLSX, etc)
- Microsoft Project
- Microsoft Visio

17.1 Filtering blocked phrases within attachments

This section contains two examples of how you can define policies to filter attachments which contain blocked phrases.

1. Identify attachments containing the word "Confidential". You do this by defining a *string of text* as a blocked phrase.
2. Identify attachments containing credit card numbers in the format "1234 1234 1234 1234" or "1234123412341234". You do this by defining a *regular expression* as a blocked phrase.

17.1.1 Filtering blocked phrases - strings of text

To define a string of text as a blocked phrase:

1. In the console tree, click **Configuration | Transport (SMTP) Scanning Policy**, and then click **Content**.
2. In the **Content filtering** dialog box, ensure that the status icons for inbound, outbound and internal messages title bars are Green and display **ON**.
3. Under **Outbound messages**, select the **On blocked phrase** check box.
4. Under **Outbound messages | On blocked phrase**, click **Define**.
5. On the **String (wildcards supported)** tab, click **Add**.
6. Click in the **Phrase** box and type `Confidential`.
7. Make sure that the **Attachment** check box is selected.

8. Click **OK** to save your changes and return to the **Content filtering** dialog box.
9. Under **Outbound messages**, click the **On blocked phrase** drop-down list and select **Quarantine message and deliver**.
10. In the **Manage changes** menu, click **Save changes**.

17.1.2 Filtering blocked phrases - regular expressions

To define a regular expression as a blocked phrase:

1. In the console tree, click **Configuration | Transport** (**SMTP**) **Scanning Policy**, and then click **Content**.
2. In the **Content filtering** dialog box, ensure that the status icons for inbound, outbound and internal messages title bars are Green and display **ON**.
3. Under **Internal messages**, select the **On blocked phrase** check box.
4. Under **Internal messages | On blocked phrase**, click **Define**.
5. On the **Regular expression** tab, click **Add**.
6. Click in the **Phrase** box and type the following regular expression:

   ```
   [0-9]{4} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
   ```

   This expression will match credit card numbers in both "1234 1234 1234 1234" and "1234123412341234" formats.

7. Make sure that the **Attachment** check box is selected.
8. Click **OK** to save your changes and return to the **Content filtering** dialog box.
9. Under **Internal messages | On blocked phrase**, click **Alert**.
10. In the **Alert configuration** dialog box, select one or more check boxes to specify who will be notified in the event of PureMessage quarantining a suspicious attachment.
11. Click **OK** to save your changes and return to the **Content filtering** dialog box.
12. In the **Manage changes** menu, click **Save changes**.

You can find more information about creating regular expressions at *http://www.regular-expressions.info/*.

18 Appendix F: Database Mirroring

Database mirroring is a feature of SQL Server (available only in the Standard and Enterprise editions of SQL Server since SQL Server 2005 SP1) that provides high-availability without the need for a single-copy cluster.

To use mirrored databases with PureMessage, you must perform the following:

- *Prepare SQL Server instances* (page 43)
- *Install PureMessage with database mirroring* (page 44)
- *Configure PureMessage for database mirroring* (page 44)

18.1 Prepare SQL Server instances

Before installing PureMessage, you must prepare the SQL Server instances that will be used. A mirrored SQL database requires two or three SQL Server instances:

1. A principal server instance (data source).
2. A mirror server instance (failover partner).
3. Optionally, a witness server instance.

For information on SQL Server preparation for mirroring, see:

http://www.microsoft.com/technet/prodtechnol/sql/2005/dbmirror.mspx

http://msdn.microsoft.com/en-us/library/ms190941.aspx

Note:

- Ensure that the SQL Server instances are authenticated to access each other. This means that the accounts under which a SQL Server instances run must be granted access to the other SQL Server instances used in the mirror set, and that remote connections (e.g. over the TCP/IP protocol) must be enabled.
- The principal and mirror server instances should host the same edition of SQL Server, and it should be an edition that supports mirroring.
- For automatic failover, a witness server is required.
- For high-availability, the SQL Server instances must be installed on different physical servers and use synchronous mode.
- If any firewalls exist between the SQL Servers, they must be configured to allow the SQL servers to communicate over the TCP port chosen for mirroring.
- It is recommended that SQL installations use the same SQL instance name and file paths on all servers.

18.2 Install PureMessage with database mirroring

Database mirroring is enabled in PureMessage by selecting the **Remote** database option and supplying the names of both the principal and mirror server instances during installation. The names should be entered in the PureMessage Database settings dialog box, separated with a semi-colon.

Example: Server1\Instance1;Server2\Instance1

When the instance names are specified separated with a semi-colon, the PureMessage installer will install the SQL Server Native Client, if it is not already present on the system. If an earlier version of SQL Native Client is available, PureMessage will upgrade it to SQL Native Client for SQL Server 2008 SP1.

If PureMessage has already been installed without mirroring then these changes can be made retrospectively. For information, contact Sophos Technical Support.

18.3 Configure PureMessage for database mirroring

Once the PureMessage installation is completed, the databases and PureMessage login will have been created on the principal server instance.

The PureMessage login is named <domain>\SophosPureMessage, where <domain> is the domain of the PureMessage Server (or the machine name for a server that is in a workgroup).

The following steps can all be performed from the SQL Server Management Studio application, or by issuing the SQL commands provided:

For more information on using SQL Server Management Studio see, *http://technet.microsoft.com/en-us/library/ms175134.aspx*.

1. Create the PureMessage login on the mirror server instance:

   ```
   [Mirror]> CREATE LOGIN [<domain name>\SophosPureMessage] FROM
   WINDOWS
   ```

   `<domain name>` must be replaced with the actual domain of your PureMessage server, or with the machine name if in a Workgroup.

   For more information on setting up login accounts, see *http://technet.microsoft.com/en-us/library/ms366346.aspx*.

2. Perform a full backup for each of the four PureMessage databases from the principal server:

```
[Principal]> BACKUP DATABASE [SavexCnfg] TO DISK =
'<path>\SavexCnfg.bak'
[Principal]> BACKUP DATABASE [SavexDir] TO DISK =
'<path>\SavexDir.bak'
[Principal]> BACKUP DATABASE [SavexQuar] TO DISK =
'<path>\SavexQuar.bak'
[Principal]> BACKUP DATABASE [SavexRprt] TO DISK =
'<path>\SavexRprt.bak'
```

   `<path>` must be replaced with a path to a folder where the backup is to be stored.

   For more information on preparing a mirror database for mirroring, see *http://technet.microsoft.com/en-us/library/ms189047.aspx*.

3. Make the database backup available on the mirror server and restore each database to the mirror server instance. This will set the mirrored databases to **Mirror, Synchronized/Restoring** state.

```
[Mirror]> RESTORE DATABASE [SavexCnfg] FROM DISK =
'<path>\SavexCnfg.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexDir] FROM DISK =
'<path>\SavexDir.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexQuar] FROM DISK =
'<path>\SavexQuar.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexRprt] FROM DISK =
'<path>\SavexRprt.bak' WITH NORECOVERY
```

   `<path>` must be replaced with a path to a folder where the backup is held.

   If the path names of the principal and mirror databases differ then it will be necessary to use the MOVE option of the RESTORE command, e.g.

```
[Mirror]> RESTORE DATABASE [SavexCnfg] FROM DISK =
<path>\SavexCnfg.bak' WITH NORECOVERY,
MOVE 'SavexCnfg' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\DATA\SavexCnfg.mdf',
MOVE 'SavexCnfg_log' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\DATA\SavexCnfg_1.LDF'
```

   For more information on preparing a mirror database for mirroring, see *http://technet.microsoft.com/en-us/library/ms189047.aspx*.

4. Create a mirroring endpoint on the principal server instance:

```
[Principal]> CREATE ENDPOINT [Mirroring]
STATE=STARTED
AS TCP (LISTENER_PORT = <port>)
FOR DATA_MIRRORING (ROLE = PARTNER)
```

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

5. Create an endpoint on the mirror server instance:

```
[Mirror]> CREATE ENDPOINT [Mirroring]
STATE=STARTED
AS TCP (LISTENER_PORT = <port>)
FOR DATA_MIRRORING (ROLE = ALL)
```

6. Point the mirror server instance's partner to the principal server instance:

```
[Mirror]> ALTER DATABASE [SavexCnfg] SET PARTNER =
'TCP://<hostname>:<port>'
[Mirror]> ALTER DATABASE [SavexDir] SET PARTNER =
'TCP://<hostname>:<port>'
[Mirror]> ALTER DATABASE [SavexQuar] SET PARTNER =
'TCP://<hostname>:<port>'
[Mirror]> ALTER DATABASE [SavexRprt] SET PARTNER =
'TCP://<hostname>:<port>'
```

   `<hostname>` must be replaced with the fully-qualified, DNS hostname of the principal server.

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

7. Point the principal server instance's partner to the mirror server instance:

```
[Principal]> ALTER DATABASE [SavexCnfg] SET PARTNER =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexDir] SET PARTNER =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexQuar] SET PARTNER =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexRprt] SET PARTNER =
'TCP://<hostname>:<port>'
```

   `<hostname>` must be replaced with the fully-qualified, DNS hostname of the mirror server.

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

   For more information on setting up database mirroring using Windows authentication, see *http://technet.microsoft.com/en-us/library/ms179306.aspx*.

8. If a witness server is required then it can be configured as follows:

```
[Witness]> CREATE ENDPOINT [Mirroring]
STATE=STARTED
AS TCP (LISTENER_PORT = <port>)
FOR DATA_MIRRORING (ROLE = WITNESS)
```

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

9. If a witness server is required on the principal server, set the witness for each database:

```
[Principal]> ALTER DATABASE [SavexCnfg] SET WITNESS =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexDir] SET WITNESS =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexQuar] SET WITNESS =
'TCP://<hostname>:<port>'
[Principal]> ALTER DATABASE [SavexRprt] SET WITNESS =
'TCP://<hostname>:<port>'
```

   `<hostname>` must be replaced with the fully-qualified, DNS hostname of the witness server.

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

   For more information on adding a database mirroring witness using Windows authentication, see *http://technet.microsoft.com/en-us/library/ms190430.aspx*.

10. Depending on the permissions of the accounts running the SQL servers it may be necessary to explicitly grant permissions to the accounts for accessing the endpoints as follows:

```
[Principal]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
[Mirror]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
[Witness]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
```

   `<user>` must be replaced with the SAM name of account running the accessing SQL Server.

11. If necessary, e.g. if the servers are under heavy load, increase the ping timeout for the connections as follows:

```
[Principal]> ALTER DATABASE [SavexCnfg] SET PARTNER TIMEOUT
<integer>
[Principal]> ALTER DATABASE [SavexDir] SET PARTNER TIMEOUT
<integer>
[Principal]> ALTER DATABASE [SavexQuar] SET PARTNER TIMEOUT
<integer>
[Principal]> ALTER DATABASE [SavexRprt] SET PARTNER TIMEOUT
<integer>
```

   `<integer>` must be replaced with the required timeout (in seconds). The default time out used by SQL Server is 10 seconds.

19 Glossary

Active Directory synchronization	A one-way synchronization of Active Directory users and groups with the PureMessage cache.
Active/Passive cluster	A two-node cluster where the Active node owns the services and the Passive node remains inoperative.
adware and PUAs	Adware displays advertising, for example, pop-up messages, which affects user productivity and system efficiency. A potentially unwanted application (PUA) is an application that is not inherently malicious but is generally considered unsuitable for the majority of business networks.
background scanning	A form of scanning in which the Exchange Store is scanned when the Exchange server has periods of low activity.
dashboard	An at-a-glance view of the status of the PureMessage servers.
demilitarized zone (DMZ)	A network area protected by firewalls that sits between an organization's internal network and an external network, usually the internet.
downstream	A transmission from an information server toward an end user.
email relay	A type of server used to pass email from one point of the internet to another. Every email contains a list of the email relays it passes through on the internet, including the relay that was used to send the email.
Exchange Store	The mailbox and public folders stored on an Exchange server.
failover	In an Active/Passive cluster, the capability to switch services automatically to the Passive node upon the failure or abnormal termination of the Active node.
information store	See Exchange store.
malware	Short for malicious software. Software designed specifically to damage or disrupt a system, such as a virus, worm, or Trojan.
node	A server that is part of a cluster.
non-delivery report (NDR)	An automated electronic mail message from a mail system to a sender indicating failed message delivery.
on-access scanning	A form of real-time scanning in which new items in the Exchange Store are scanned as soon as they are accessed by an email client.

private store	A database (usually a mailbox) on an Exchange server that is only accessible to a single user.
proactive scanning	A form of real-time scanning in which new items added to the Exchange Store are added to a queue for scanning.
public store	A database on an Exchange server that is accessible to multiple users.
real-time scanning	Automatic interception and scanning of email attachments as they are sent or received.
scheduled scan	A scan that is scheduled to take place automatically at a particular time.
Simple Exchange organization	A single Exchange 2007 server that provides all Exchange services and stores all Exchange data for the entire organization.
Simple Mail Transfer Protocol (SMTP)	An internet standard for email transmission across IP networks. Email server software uses SMTP to send and receive mail messages.
spyware	A program that installs itself onto a user's computer by stealth, subterfuge, or social engineering, and sends information from that computer to a third party without the user's permission or knowledge.
upstream	A transmission from an end user toward the server.
upstream trusted relay	A known email server that sends or forward emails to the server on which PureMessage is installed.

20 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *http://community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *http://www.sophos.com/support/*.
- Download the product documentation at *http://www.sophos.com/support/docs/*.
- Send an email to *support@sophos.com*, including the following information:
  - Sophos software version number(s)
  - Mail server or gateway details
  - Operating system(s) and patch level(s)
  - The exact text of any error messages

21 Legal notices

Copyright © 2010 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

XPExplorerBar

Copyright © 2004-2005, Mathew Hall

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.